



# FortiNAC - Corporate User Device Use Case

Version F 7.2.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)

October 13, 2023

FortiNAC F 7.2.0 Corporate User Device Use Case

49-20-748677-20210922

---

## TABLE OF CONTENTS

<b>Overview .....</b>	<b>4</b>
<b>Configure FortiNAC to automatically register the endpoint device .....</b>	<b>5</b>
<b>Mapping logical networks to VLAN's .....</b>	<b>8</b>

# Overview

When FortiNAC is first deployed, after the initial discovery of infrastructure devices and endpoint devices, all endpoint devices are initially classified as rogue devices. It is important to identify corporate owned and managed devices and distinguish them from rogue devices.

The preferred method is to deploy the FortiNAC Persistent Agent on endpoint devices. Once the agent is installed, it will communicate with the FortiNAC server when it is connected to the network. For information on deploying a persistent agent, see [Persistent Agent Deployment and Configuration](#).

The FortiNAC should be configured to automatically register endpoint devices. When an endpoint device with Persistent Agent communicates with the FortiNAC server, the FortiNAC will apply its policy configuration to register the endpoint as a corporate owned or managed device.

Ideally, an endpoint device is associated *with* a logged-on user, so access can be granted based on group membership. For an endpoint device *without* a logged-on user, access should be granted through the creation of a separate Network Access Policy.

This guide shows how to create network access policies to manage corporate-owned devices, for endpoint devices with a logged-on user.

## Secondary methods to register the endpoint device

If the customer does not wish to use the Persistent Agent, there are other ways to register corporate owned endpoint devices.

1. **Run the Passive Agent with a login script / Group Policy Object:** The corporate device is automatically registered when the script runs the agent executable.
2. **802.1X auto-registration:** If the corporate machine connects to the network via 802.1X, the 802.1X auto-registration option can be used.
3. **FortiClient EMS:** If the customer has FortiClient EMS, or another MDM, devices and machines managed by the MDM will be automatically registered.

# Configure FortiNAC to automatically register the endpoint device

Configure FortiNAC to automatically register the endpoint using Persistent Agent.

Environment: The endpoint device has the Persistent Agent installed and is communicating with the FortiNAC server. We need to set up FortiNAC to register those endpoint devices.

Step 1: Set up a policy for the Persistent Agent

Step 2: Configure the network access policy

## Step 1: Set up a policy for the Persistent Agent

1. Go to **System > Settings > Persistent Agent > Credential Configuration**.
2. Enable **Registration**. Enable **Register As Device**. Authentication Type should be **LDAP**.

This tells FortiNAC to automatically register the device when the Persistent Agent talks to FortiNAC. The Register As Device box registers the device without an owner.

3. Click **Save Settings**.
4. Now you need to configure the Passive Agent to track the logged-on user. Go to **Policy & Objects > Passive Agent**. Click **Add**.
5. **Enable** the Configuration. Set the Name: "Track Logged On User."

This configuration makes FortiNAC associate a logged-on user to the appropriate device when the Persistent Agent detects an Active Directory Login. Click **Enable**. Then click **OK**.

The Passive Agent Configuration triggers FortiNAC to associate a logged-on user to the device when the Persistent Agent detects an Active Directory Login. This logged-on user can be part of a User/Host Profile and a Network Access Policy to provide network access based on a user's group membership in the Active Directory.

## Step 2: Create Network Access Policies

Network access policies work by mapping logical networks to VLANs that are defined in FortiGate. You can set up a variety of network access policies to fit your needs.

For example, you can create a "Marketing" network access policy to grant marketing staff a different network access than human resources.

The following steps show how to define a Corporate Device Network Access policy.

### Creating a Corporate Device Network Access policy

1. Go to **Policy & Objects > Network Access**. Click **Add**.
2. Set the Name, for example "Corporate Device Network Access Policy." **Enable** the policy.  
Add a User/Host Profile.  
Name: "Corporate Device Profile"  
Where (Location): Any  
Who/What by Group: Any  
Who/What by Attribute: Host [Persistent Agent: Yes]. Click **Add**. Select the **Host** tab. Enable **Persistent Agent**. Click **OK**.

**Modify User/Host Profile**

Name: Corporate Device Profile

Where (Location): Any Select...

Who/What by Group: Any Select...

Who/What by Attribute: Host [Persistent Agent: Yes] Add Modify Delete

Who/What by RADIUS Request Attribute: Add Modify Delete

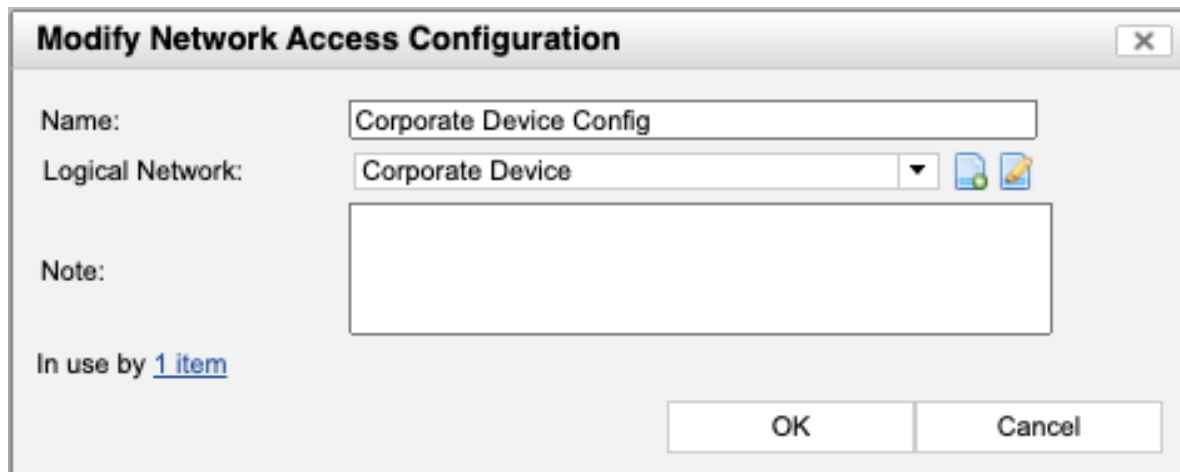
When: Always

Note:

In use by [2 items](#)

OK Cancel

3. Click **OK**.
4. Add a Network Access Configuration.
5. Set the name for the configuration.  
Logical Network: Use an existing logical network or create one.



**Modify Network Access Configuration**

Name: Corporate Device Config

Logical Network: Corporate Device

Note:

In use by [1 item](#)

OK Cancel

Logical Network Mapping to VLAN – For the FortiGate, the Logical Network “Corporate Device” is mapped to VLAN 140.

6. Click **OK**.

## Mapping logical networks to VLAN's

For all the locations where you want to enable this policy, you must map the logical network to a VLAN.

1. Go to **Network > Inventory > Containers**.
2. Select the relevant device. Depending on your device, steps may differ. Select the Model Configuration, and map the logical networks to the appropriate VLAN's.

### Setting up a network access policy for marketing

#### Steps

1. Go to **Policy & Objects > Network Access**. Click **Add**.
2. Set the Name, for example "Marketing Group." Enable the policy.
3. Create a User/Host Profile by clicking the Add button
  - a. Name: "Marketing Group Profile"
  - b. Where (Location): Any
  - c. Who/What by Group: Any
  - d. Who/What by Attribute: Persistent Agent: Yes
4. Add a Network Access Configuration.
  - a. Set the name for the configuration.
  - b. Logical Network: Use an existing logical network or create one.

Click **OK**

#### Mapping logical networks to VLAN's

Define the Logical Network as "Marketing".

For all the locations where you want to enable this policy, you must map the logical network to a VLAN.

1. Go to **Network > Inventory**.
2. Select the relevant device. Select the Model Configuration and map the logical networks to the appropriate VLAN's.

For the FortiGate, the Logical Network "Marketing" is mapped to VLAN 162



**Network Access**VLAN Display Format: ☒ VLAN Name ☐ VLAN ID ☐ Manual

Default	Enforce ▼	VLAN_162 ▼	Dead End	Enforce ▼	VLAN_99 ▼
Registration	Enforce ▼	VLAN_99 ▼	Quarantine	Enforce ▼	VLAN_99 ▼
Authentication	Enforce ▼	(None) ▼	Corporate Device	Enforce ▼	VLAN_140 ▼
Guest	Enforce ▼	VLAN_150 ▼	IP Camera	Enforce ▼	VLAN_200 ▼
UPS	Enforce ▼	(None) ▼	Contractor	Enforce ▼	(None) ▼
BYOD	Enforce ▼	VLAN_150 ▼	PLC	Enforce ▼	VLAN_77 ▼
HMI	Enforce ▼	(None) ▼	RTU	Enforce ▼	(None) ▼
DeadEnd	Enforce ▼	VLAN_99 ▼	Marketing	Enforce ▼	VLAN_162 ▼

Note: The list of VLANs available represents those VLANs that are common to all devices of this vendor type.

This example has a policy for Corporate Devices, as well as a policy for the Marketing department.

**Example of Network Access Policies**

Network Access Policies - Total: 14						
Rank:   Set Rank		Enable:				
Rank	Enabled	Name	User/Host Profile	Network Access Configuration	Last Modified By	Last Modified Date
1		Marketing Staff Policy	<a href="#">Marketing Profile</a>	<a href="#">Marketing Configuration</a>	admin	2023/09/13 13:44:04
2		Corporate Device Policy	<a href="#">Corporate Device Profile</a>	<a href="#">Corporate Device Config</a>	admin	2023/09/13 13:44:04
3		Contractor Policy	<a href="#">Contractor Profile</a>	<a href="#">Contractor</a>	admin	2023/07/27 14:17:19
4		Non Communicating PA Policy	<a href="#">Non Communicating PA Profile</a>	<a href="#">Dead End Configuration</a>	admin	2023/07/27 14:17:19
5		IP Camera Policy	<a href="#">IP Camera Profile</a>	<a href="#">IP Camera Config</a>	admin	2023/07/27 14:17:19
6		UPS Policy	<a href="#">UPS Profile</a>	<a href="#">UPS Config</a>	admin	2023/07/27 14:17:19
7		HMI Policy	<a href="#">HMI Profile</a>	<a href="#">HMI Config</a>	admin	2023/07/27 14:17:19
8		PLC Policy	<a href="#">PLC Profile</a>	<a href="#">PLC Configuration</a>	admin	2023/07/27 14:17:18
9		Remote Terminal Unit Policy	<a href="#">RTU Profile</a>	<a href="#">RTU Config</a>	admin	2023/07/27 14:17:18
10		Faculty BYOD Policy	<a href="#">BYOD Profile</a>	<a href="#">BYOD</a>	admin	2023/07/05 12:33:07
11		Student BYOD Policy	<a href="#">BYOD Profile</a>	<a href="#">BYOD</a>	admin	2023/07/05 12:33:06
12		Guest Device Policy	<a href="#">Guest Device Profile</a>	<a href="#">Guest Device Config</a>	admin	2023/07/05 12:33:06
13		BYOD Policy	<a href="#">BYOD Profile</a>	<a href="#">BYOD</a>	admin	2022/10/26 13:58:47
14		Corporate Device Network Access Policy	<a href="#">Corporate Device Profile 2</a>	<a href="#">Corporate Device config 2</a>	admin	2023/08/30 14:31:17

The Marketing policy is ranked higher than the Corporate Device policy because it is more specific.



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.